UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

IN RE PEOPLES BANK, AS A SUCCESSOR TO LIMESTONE BANK, DATA BREACH LITIGATION	**Case No. 2:23-CV-03043** **Distrct Judge Michael H. Watson** **Magistrate Judge Elizabeth P. Deavers** **CONSOLIDATED AMENDED CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Latasha Brooks, Michael Brooks, Earl Blankenship, Stephen McDonald, and Cheryl Barefoot (collectively, "Plaintiffs") bring this Class Action Complaint ("Complaint") against Defendant Peoples Bank as successor by merger to Limestone Bank, Inc. ("Defendant"), an Ohio corporation, individually and on behalf of all others similarly situated ("Class Members"), and allege, upon personal knowledge as to their own actions and their counsel's investigations, and upon information and belief as to all other matters as follows:

INTRODUCTION

1. Defendant experienced a cyberattack at an undisclosed point in time between November 21, 2022, and March 23, 2023 (the "Data Breach"). Plaintiffs bring this class action against Defendant on behalf of themselves and approximately 47,000 Class Members for Defendant's failure to properly secure and safeguard personally identifiable information, including: name, date of birth, address, Social Security number, and financial account number (collectively, "Private Information").

2. Defendant maintained Plaintiffs' and Class Members' Private Information in a reckless manner. In particular, the Private Information was maintained on Defendant's computer system and network in a condition vulnerable to cyberattacks. Upon information and belief, the mechanism of the cyberattack and potential for improper disclosure of Plaintiffs' and Class Members' Private Information was a known risk to Defendant, and thus Defendant was on notice that failing to take steps necessary to secure the Private Information from those risks left that property in a dangerous condition.

3. The Private Information that was stolen is one-stop shopping for identity thieves to wreak complete havoc on their victims' lives. Armed with the Private Information accessed in the Data Breach, data thieves can commit a variety of crimes including, e.g., opening new financial accounts in Class Members' names or accessing existing accounts, taking out loans in Class Members' names, using Class Members' names to obtain medical services, using Class Members' information to obtain government benefits, filing fraudulent tax returns using Class Members' information, obtaining driver's licenses in Class Members' names but with another person's photograph, and giving false information to police during an arrest. Given the sensitivity and static nature of the Private Information involved (such as names, Social Security numbers, and medical information), Plaintiffs and Class Members will be forced to live in fear the rest of their lives.

4. The substantial risk of harm from the Data Breach has caused Plaintiffs and Class Members to incur losses of time, out-of-pocket expenses (e.g., credit monitoring services), and to suffer fear, stress, and anxiety. As a result of having their Private Information acquired by cybercriminals, Plaintiffs and Class Members have also suffered invasions of privacy, and many have suffered instances of actual theft, fraud, and other misuse of Private Information.

5. Plaintiffs bring claims against Defendant for: (i) negligence, (ii) negligence per se;

(iii) unjust enrichment, (iv) breach of implied contract, (v) breach of fiduciary duty, and (vi) declaratory and injunctive relief.

6. Plaintiffs seek remedies on behalf of themselves and the Class Members, including, but not limited to, nominal, compensatory, and punitive damages, as well as injunctive and declaratory relief regarding the need for continued credit monitoring and the continued inadequacy of Defendant's data security policies, procedures, and protections.

THE PARTIES

7. Plaintiff Latasha Brooks is, and at all times mentioned herein was, an individual citizen of the State of Kentucky. Plaintiff Latasha Brooks was notified of the Data Breach and her Private Information being compromised upon receiving a data breach notice letter dated on or around September 15, 2023.

8. Plaintiff Michael Brooks is, and at all times mentioned herein was, an individual citizen of the State of Kentucky. Plaintiff Michael Brooks was notified of the Data Breach and his Private Information being compromised upon receiving a data breach notice letter dated on or around September 15, 2023.

9. Plaintiff Earl Blankenship is, and at all times mentioned herein was, an individual citizen of the State of Kentucky. Plaintiff Blankenship was notified of the Data Breach and his Private Information being compromised upon receiving a data breach notice letter dated on or around September 15, 2023.

10. Plaintiff Stephen McDonald is, and at all times mentioned herein was, an individual citizen of the State of Kentucky. Plaintiff Stephen McDonald was notified of the Data Breach and his Private Information being compromised upon receiving a data breach notice letter dated on or around September 15, 2023.

11. Plaintiff Cheryl Barefoot is, and all times mentioned herein was, an individual

citizen of the State of Kentucky. Plaintiff Barefoot was notified of the Data Breach and her Private Information being compromised upon receiving a data breach notice letter dated on or around September 15, 2023.

12. Defendant is an Ohio corporation and chartered commercial bank with its principal office located at 138 Putnam St., Marietta, OH 45750. It operates 132 full-service branch locations throughout Ohio, Kentucky, West Virginia, Washington D.C., and Maryland.

13. Limestone Bank, Inc., a former Kentucky banking corporation, merged with and into Peoples Bank on April 30, 2023, at which point its corporate existence ceased and "all, debts liabilities and duties of Limestone…bec[a]me obligations of [Defendant], and may [now] be enforced against it to the same extent as if such debts, liabilities and duties had been incurred or contracted by it."[1] Plaintiffs' claims stated herein are therefore asserted against Defendant as successor by merger to Limestone Bank, Inc.

14. At the time of filing its Articles of Merger with the Kentucky Secretary of State, Defendant also adopted "Limestone Bank, Inc." as an assumed name for use in the Commonwealth of Kentucky with effect from May 1, 2023, and therefore all actions taken in the name of Limestone Bank, Inc., on and after that date have been taken by Defendant.[2] Said differently, any action brought against Limestone Bank, Inc. is also brought against Defendant.

15. The true names and capacities of persons or entities, whether individual, corporate,

[1] Articles of Merger of Limestone Bank, Inc., a Kentucky Banking Corporation, with and into Peoples Bank, an Ohio Chartered Commercial Bank, Ex. A (Form of Agreement and Plan of Merger), at Agreements, § 9 (Apr. 28, 2023), filed with the Kentucky Secretary of State and available at his official website here: https://web.sos.ky.gov/corpscans/84/0950084-09-99999-20230428-9585781-PU.pdf (last visited Jan. 19, 2024).

[2] Certificate of Assumed Name (Apr. 28, 2023) filed with the Kentucky Secretary of State and available at his official website here: https://web.sos.ky.gov/corpscans/84/0950084-09-99999-20230428-9585697-PU.pdf (last visited Jan. 19, 2024).

associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties if and when their identities become known.

16. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

JURISDICTION & VENUE

17. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member is a citizen of a state different from Defendant to establish minimal diversity. Indeed, all Plaintiffs are of diverse citizenship from Defendant.

18. The Southern District of Ohio has personal jurisdiction over Defendant named in this action because Defendant has its principal place of business in Washington County in this District, and Defendant conducts substantial business in Ohio and this District through its headquarters, other offices, parent, and affiliates.

19. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant and/or its parents or affiliates are headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

Defendant's Business

20. Defendant is a bank headquartered in Marietta, Ohio. According to its website, it holds nearly $9 billion in total assets, consists of 132 operating full-service bank branch locations, and employs more than 1,500 associates.

21. As of March 31, 2023, Defendant had approximately $1.5 billion in total assets, and operated 20 branches throughout Kentucky.[4]

22. Through its operation, Defendant provides banking services to its clients—i.e., Plaintiffs and Class Members.

23. In order to receive banking services from Defendant, clients (i.e., Plaintiffs and Class Members) provide their Private Information to Defendant.

24. Plaintiffs and Class Members only provide their Private Information on the reasonable expectation that Defendant (a sophisticated company) will utilize any and all reasonable measures to keep their Private Information confidential. Specifically, Plaintiffs and Class Members expect Defendant to maintain its system security; to use this information for business purposes only; and to make only authorized disclosures of their Private Information. It is common sense that customers expect reasonable security when entrusting a company with highly sensitive Private Information like a combination of their names, Social Security numbers, and financial account numbers.

25. Defendant had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' Private Information from involuntary disclosure to third parties.

26. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their Private Information and would not have entrusted Defendant or Defendant's clients with their information had they known that Defendant would fail to safeguard this information from foreseeable threats.

[4] https://www.prnewswire.com/news-releases/peoples-bancorp-completes-acquisition-of-limestone-bancorp-301811352.html (last visited Jan. 19, 2024).

The Data Breach

27. On or around September 15, 2023, Defendant began notifying certain Class Members of the Data Breach.[5]

28. Between November 21, 2022, and March 23, 2023, a third party gained unauthorized access to one of Defendant's employees' email accounts. [6]

29. The Private Information compromised in the Data Breach, included individuals' names, Social Security number, and financial account information.

30. Plaintiffs and Class Members provided their Private Information, directly or indirectly, to Defendant with the reasonable expectation and mutual understanding that Defendant would comply with its obligations to keep such information confidential and secure from unauthorized access. Plaintiffs and Class Members also understood that if their Private Information was stolen, they would be notified within a reasonable amount of time.

31. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach. Defendant's negligence in safeguarding the Private Information of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to companies like Defendant to protect and secure the sensitive data they possess.

---

[5] Peoples Bank, *Limestone Security Incident Notice*, originally published at www.peoplesbancorp.com (last visited September 21, 2023), and now archived at https://web.archive.org/web/20231003172047/https://www.peoplesbancorp.com/about-us/limestone-bank/limestone-security-incident-notice (last visited Jan. 19, 2024).

[6] *Id.*

32. Therefore, the increase in such attacks and the attendant risk of future attacks were widely known to the public and to anyone in Defendant's industry, including Defendant.

Defendant's Breach of its Data Security Obligations to Plaintiffs and Class Members

33. Defendant could have prevented this Data Breach by properly securing and encrypting the files containing the Private Information of Plaintiffs and Class Members. Alternatively, Defendant should have destroyed data that it no longer needed.

34. Defendant breached its obligations to Plaintiffs and Class Members and/or was otherwise negligent and reckless because it failed to properly maintain and safeguard its computer systems and data. Defendant's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber-attacks;

b. Failing to adequately protect customers' Private Information;

c. Failing to properly monitor its own data security systems for existing intrusions;

d. Failing to ensure that its vendors with access to its computer systems and data employed reasonable security procedures;

e. Failing to train its employees in the proper handling of emails containing Private Information and maintain adequate email security practices;

f. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act;

g. Failing to adhere to industry standards for cybersecurity; and

h. Waiting almost two years to notify Plaintiffs and Class Members that their Private Information was compromised in the Data Breach.

35. Defendant negligently and unlawfully failed to safeguard Plaintiffs' and Class Members' Private Information by allowing cyberthieves to access Defendant's computer network and systems which contained unsecured and unencrypted Private Information.

Defendant Fails to Comply with FTC Guidelines

36. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

37. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cyber-security guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct any security problems.[7] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[8]

38. The FTC further recommends that companies not maintain Private Information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

39. The FTC has brought enforcement actions against businesses for failing to

---

[7] *Protecting Personal Information: A Guide for Business*, Federal Trade Commission (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Jan. 19, 2024).

[8] *Id*.

adequately and reasonably protect customer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

40. Defendant failed to properly implement basic data security practices.

41. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to individuals' Private Information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

42. Defendant was at all times fully aware of its obligation to protect the Private Information obtained from its customers. Defendant was also aware of the significant repercussions that would result from its failure to do so.

Defendant Fails to Comply with Industry Standards

43. As shown above, experts studying cyber security routinely identify entities operating in banking as being particularly vulnerable to cyberattacks because of the value of the Private Information which they collect and maintain.

44. Several best practices have been identified that a minimum should be implemented by entities like Defendant, including, but not limited to, the following: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and anti-malware software; encryption, making data unreadable without a key; multi-factor authentication; backup data, and; limiting which employees can access sensitive data.

45. Other best cybersecurity practices that are standard in the legal industry include installing appropriate malware detection software; monitoring and limiting the network ports;

protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system; training staff regarding critical points.

46. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

47. These foregoing frameworks are existing and applicable industry standards in the banking industry, and Defendant failed to comply with these accepted standards, thereby opening the door to the cyber incident and causing the data breach.

Plaintiffs and Class Members Face a Substantial Risk of Increased Harm

48. Victims of all data breaches are exposed to serious ramifications regardless of the nature of the data. Indeed, the reason criminals steal personally identifiable information is to monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity thieves who desire to extort and harass victims, take over victims' identities in order to engage in illegal financial transactions under the victims' names. Because a person's identity is akin to a puzzle, the more accurate pieces of data an identity thief obtains about a person, the easier it is for the thief to take on the victim's identity, or otherwise harass or track the victim.

49. For example, armed with just a name and date of birth, a data thief can utilize a hacking technique referred to as "social engineering" to obtain even more information about a victim's identity, such as a person's login credentials or Social Security number. Social

engineering is a form of hacking whereby a data thief uses previously acquired information to manipulate individuals into disclosing additional confidential or personal information through means such as spam phone calls and text messages or phishing emails.

50. Here, the cybercriminals targeted and successfully exfiltrated Social Security numbers, which are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult, if not impossible, for an individual to change. Identity thieves use Social Security numbers for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud. Identity thieves also use Social Security numbers to obtain a driver's license or official identification card in the victim's name but with the thief's picture; use the victim's name and Social Security number to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's Social Security number, rent a house or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest resulting in an arrest warrant being issued in the victim's name.

51. The Social Security Administration stresses that the loss of an individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[9]

52. It is incredibly difficult to change or cancel a stolen Social Security number. An

[9] Social Security Administration, *Identity Theft and Your Social Security Number* (July 2021), https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited Jan. 19, 2024).

individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

53. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[10]

54. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, only credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach, including Social Security number and name, is impossible to "close" and difficult, if not impossible, to change.

55. Criminals are also able to piece together bits and pieces of compromised Private Information for develop what are called "Fullz" packages.[11]

---

[10] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last visited Jan. 19, 2024).

[11] "Fullz" is fraudster-speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off of those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014),

56. With "Fullz" packages, cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

57. The development of "Fullz" packages means here that the stolen Private Information from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

58. The existence and prevalence of "Fullz" packages means that the Private Information stolen from the data breach can easily be linked to the unregulated data of Plaintiffs and the other Class Members. Cybercriminals can then use this information to misrepresent their identity to gain access to financial and other accounts by providing verifying information compiled from unique sources.

59. Thus, even if certain information was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package.

60. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to identity thieves and other criminals (like illegal and scam telemarketers).

61. The FTC recommends that identity theft victims take several steps to protect their

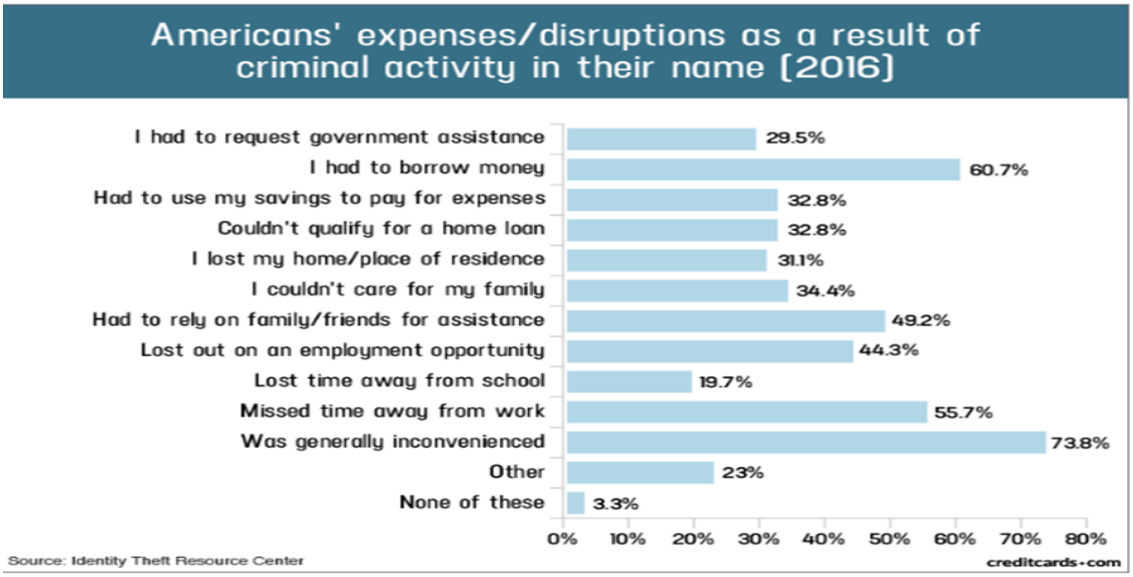
---

https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/ (last visited on Jan. 19, 2024).

personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[12]

62. The United States Government Accountability Office released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[13]

63. A study by Identity Theft Resource Center shows the multitude of harms caused by fraudulent use of personal and financial information:[14]



[12] *See IdentityTheft.gov*, Federal Trade Commission, https://www.identitytheft.gov/Steps (last visited Jan. 19, 2024).

[13] *See* U.S. Gov. Accounting Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (2007), https://www.gao.gov/new.items/d07737.pdf (last visited Jan. 19, 2024).

[14] *See* Jason Steele, *Credit Card and ID Theft Statistics*, CreditCards.com (Oct. 23, 2020) https://www.creditcards.com/statistics/credit-card-security-id-theft-fraud-statistics-1276/ (last visited Jan. 19, 2024).

64. It must also be noted there may be a substantial time lag – measured in years – between when harm occurs and when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used.

65. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

See GAO Report, at p. 29.

66. Plaintiffs and Class Members must vigilantly monitor their financial and other accounts for many years to come. Yet, to date, Defendant has only offered Plaintiffs and Class Members temporary, non-automatic credit monitoring despite Plaintiffs and Class Members being forced to face a lifetime of risk of their financial information being compromised as a result of their sensitive, Private Information being exfiltrated in the Data Breach. Defendant's offer of temporary credit monitoring indicates that even Defendant understands that Plaintiffs and Class Members now face a present and increased risk of harm due to their Private Information being exfiltrated from Defendant's systems by criminal threat actors.

The Value of Private Information

67. Private Information is an extremely valuable property right.[15]

68. Its value is axiomatic, considering the value of "big data" in corporate America and

[15] *See, e.g.*, John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

the fact that the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that Private Information has considerable market value.

69. Sensitive Private Information can sell for as much as $363 per record according to the Infosec Institute.[16] Other studies show that personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[17] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[18] Criminals can also purchase access to entire company data breaches from $900 to $4,500.

70. Static information that does not change like names, Social Security numbers, and health information, is particularly valuable. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "[c]ompared to credit card information, personally identifiable information and Social Security Numbers are worth more than 10x on the black market."[19]

71. An active and robust legitimate marketplace for Private Information also exists. In 2021, the data brokering industry was worth roughly $200 billion.[20] In fact, the data marketplace

---

[16] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, InfoSec (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/ (last visited Jan. 19, 2024).

[17] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last visited Jan. 19, 2024).

[18] Experian, *Here's How Much Your Personal Information Is Selling for on the Dark Web* (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Jan. 19, 2024).

[19] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, originally published at Computer World, www.itworld.com (Feb. 6, 2015), now at https://web.archive.org/web/20230526051155/https://www.computerworld.com/article/2880960/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited Jan. 19, 2024).

[20] https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited January 17, 2024).

is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[21,22] Consumers who agree to provide their web browsing history to the Nielsen Corporation can receive benefits worth up to $50.00 a year.[23] Users of the personal data collection app Streamlytics can earn up to $200 a month by selling their personal information to marketing companies who use it to build consumer demographics profiles.[24]

72. Consumers also recognize the value of their personal information and offer it in exchange for goods and services. The value of Private Information can be derived not by a price at which consumers themselves actually seek to sell it, but rather in the economic benefit consumers derive from being able to use it and control the use of it. For example, Plaintiffs and Class Members were only to obtain services from Defendant or Defendant's clients after providing their Private Information. A consumer's ability to use their Private Information is encumbered when their identity or credit profile is infected by misuse or fraud. For example, a consumer with false or conflicting information on their credit report may be denied credit. In this sense, among others, the theft of Private Information in the Data Breach led to a diminution in value of the Private Information.

73. As a result of the Data Breach, Plaintiffs' and Class Members' Private Information, which has an inherent market value in both legitimate and dark markets, has been damaged and

---

[21] https://datacoup.com/ (last visited January 17, 2024).

[22] *Sell your personal data? We've got a better idea…-Digi.me* (Nov. 27, 2015), https://blog.digi.me/2015/11/27/sell-your-personal-data-weve-got-a-much-better-idea-than-that/ (last visited Jan. 19, 2024).

[23] The Nielsen Company (US), LLC, *Computer & Mobile Panel Frequently Asked Questions*, https://computermobilepanel.nielsen.com/ui/US/en/faqen.html (last visited Jan. 19, 2024).

[24] How To Sell Your Own Data And Why You May Want to, available at https://www.mic.com/impact/selling-personal-data-streamlytics (last visited Jan. 19, 2024).

diminished by its compromise and unauthorized release. However, this transfer of value occurred without any consideration paid to Plaintiffs or Class Members for their property, resulting in an economic loss. Moreover, the Private Information is now readily available, and the rarity of the Data has been lost, thereby causing additional loss of value.

Plaintiffs' and Class Members' Damages

74. Plaintiffs and Class Members have been damaged by the compromise of their Private Information in the Data Breach. All Plaintiffs and Class Members have suffered losses of time, invasions of privacy, and the diminished value of their Private Information.

75. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members have been forced to spend time dealing with the effects of the Data Breach. For example, the notification letters to Plaintiffs and Class Members stated, "We encourage you to remain vigilant against identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors." Plaintiffs and Class Members will also spend significant time:

a. Reviewing and monitoring sensitive accounts and finding fraudulent insurance claims, loans, and/or government benefits claims;

b. Purchasing credit monitoring and identity theft prevention;

c. Placing "freezes" and "alerts" with reporting agencies;

d. Spending time on the phone with or at financial institutions, healthcare providers, and/or government agencies to dispute unauthorized and fraudulent activity in their name;

e. Contacting financial institutions and closing or modifying financial accounts; and,

f. Closely reviewing and monitoring Social Security Number, medical insurance accounts, bank accounts, and credit reports for unauthorized activity for years to come.

76. Plaintiffs and Class Members have incurred or will incur out-of-pocket costs for protective measures such as credit monitoring fees, credit report fees, credit freeze fees, and similar costs directly or indirectly related to the Data Breach.

77. Plaintiffs and Class Members all suffered injury from the loss of the benefit of their bargain. Specifically, Plaintiffs and Class Members provided their Private Information to Defendant with the understanding that their Private Information would be reasonably safeguarded from foreseeable threats, and that they would be notified within a reasonable amount of time if their Private Information was obtained by a third-party without authorization. Yet, this information was maintained in a negligent or reckless manner, and Defendant then waited almost two years to notify Plaintiffs and Class Members that their Private Information was compromised.

78. Plaintiffs and Class Members have also suffered fear, stress, and anxiety that is proportional to the risk of harm they face and the invasions of privacy that they have suffered.

79. Moreover, Plaintiffs and Class Members have a continuing interest in ensuring that their Private Information, which is believed to remain in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards, including but not limited to, making sure that the storage of data or documents containing Private Information is not accessible online and that access to such data is password protected.

Plaintiff Latasha Brooks' Experience

80. Plaintiff Latasha Brooks greatly values her privacy and is very careful with her Private Information. Plaintiff Latasha Brooks stores any documents containing Private Information in a safe and secure location or destroys such documents when they are no longer needed. Plaintiff Latasha Brooks has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Latasha Brooks diligently chooses

unique usernames and passwords for her various online accounts. When Plaintiff Latasha Brooks does entrust a third-party with her Private Information, it is only because she understands such information will be reasonably safeguarded from foreseeable threats, and that she will be timely notified if her data is exposed.

81. For example, Plaintiff Latasha Brooks provided her sensitive Private Information to Defendant in order to receive banking services and did so with the understanding that Defendant would safeguard it from unauthorized disclosure. Plaintiff Latasha Brooks first became a customer of Defendant's in or around August of 2004. Upon information and belief, Defendant used her Private Information when providing her with its services.

82. Plaintiff Latasha Brooks received a letter dated September 15, 2023, from Defendant notifying her of the Data Breach. The letter advised that unauthorized third parties accessed Defendant's network. The letter further advised that Plaintiff Latasha Brooks' Private Information—including her name, date of birth, address, and Social Security number,—was identified as having been "copied from [Defendant's] network."

83. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Latasha Brooks faces, the letter offered Plaintiff Latasha Brooks a 6-month subscription to credit monitoring services. The letter further instructed Plaintiff Latasha Brooks to "remain vigilant by reviewing your account statements and credit reports closely." The letter additionally encouraged Plaintiff Latasha Brooks to consider implementing the protective measures detailed in the "Steps You Can Take to Protect Your Personal Information" section of the letter.

84. As a result of the Data Breach, Plaintiff Latasha Brooks has spent approximately 24 hours researching the Data Breach, verifying the legitimacy of the notice letter, signing up for the credit monitoring service, reviewing her bank accounts, monitoring her credit report, changing

her passwords and payment account numbers, and other necessary mitigation efforts. This is valuable time Plaintiff Latasha Brooks spent at Defendant's direction and that she otherwise would have spent on other activities, including but not limited to work and/or recreation.

85. As a result of the Data Breach, Plaintiff Latasha Brooks has received an influx of spam phone calls regarding her credit report, line of credit increase, or opening a new credit card. Prior to the Data Breach, Plaintiff Latasha Brooks had never previously received spam calls regarding her credit. Plaintiff Latasha Brooks attributes these spam calls to the Data Breach because she has never knowingly been part of another Data Breach or otherwise disclosed her Private Information to unauthorized third parties. Said differently, the only way her Private Information was disclosed to third parties was through the Data Breach.

86. The Data Breach also caused Plaintiff Latasha Brooks to suffer a loss of privacy.

87. As a result of the Data Breach, Plaintiff Latasha Brooks will face a substantial risk of imminent harm for the rest of her life.

88. Plaintiff Latasha Brooks anticipates spending additional considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

89. The substantial risk of harm and loss of privacy from the Data Breach has caused Plaintiff Latasha Brooks to suffer fear, anxiety, annoyance, inconvenience, and nuisance.

90. The Data Breach caused Plaintiff Latasha Brooks to suffer a diminution in the value of her Private Information.

91. Plaintiff Latasha Brooks has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

92. As a result of the Data Breach, Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain she made with Defendant by overpaying for services that were intended to be accompanied by adequate data security but were not; (e) loss of time and effort that Plaintiff Latasha Brooks has had to expend in an attempt to ameliorate, mitigate, and address the consequences of the Data Breach, with such steps being taken at the direction of Defendant; and (f) continued risk to Plaintiff's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Michael Brooks

93. Plaintiff Michael Brooks greatly values his privacy and is very careful with his Private Information. Plaintiff Michael Brooks stores any documents containing Private Information in a safe and secure location or destroys such documents when they are no longer needed. Plaintiff Michael Brooks has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Michael Brooks diligently chooses unique usernames and passwords for his various online accounts. When Plaintiff Michael Brooks does entrust a third-party with his Private Information, it is only because he understands such information will be reasonably safeguarded from foreseeable threats, and that he will be timely notified if his data is exposed.

94. For example, Plaintiff Michael Brooks provided his sensitive Private Information to Defendant in order to receive banking services and did so with the understanding that Defendant would safeguard it from unauthorized disclosure. Plaintiff Michael Brooks first became a customer of Defendant's in or around August 2004. Upon information and belief, Defendant used his Private Information when providing him with its services.

95. Plaintiff Michael Brooks received a letter dated September 15, 2023, from Defendant notifying him of the Data Breach. The letter advised that unauthorized third parties accessed Defendant's network. The letter further advised that Plaintiff Michael Brooks' Private Information—including his name, date of birth, address, and Social Security number—was identified as having been "copied from [Defendant's] network."

96. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Michael Brooks faces, the letter offered Plaintiff Michael Brooks a 6-month subscription to credit monitoring services. The letter further instructed Plaintiff Michael Brooks to "remain vigilant by reviewing your account statements and credit reports closely." The letter additionally encouraged Plaintiff Michael Brooks to consider implementing the protective measures detailed in the "Steps You Can Take to Protect Your Personal Information" section of the letter.

97. As a result of the Data Breach, Plaintiff Michael Brooks has spent approximately 24 hours researching the Data Breach, verifying the legitimacy of the notice letter, signing up for the credit monitoring service, reviewing his bank accounts, monitoring his credit report, changing passwords and payment account numbers, and other necessary mitigation efforts. This is valuable time Plaintiff Michael Brooks spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

98. As a result of the Data Breach, a third party used Plaintiff Michael Brooks' Private

Information to attempt to open a fraudulent credit card. Plaintiff

99. As a result of the Data Breach, a third party used Plaintiff Michael Brooks' Private Information to attempt to purchase property.

100. Prior to the Data Breach, Plaintiff Michael Brooks had never experienced fraud with respect to his Private Information. Plaintiff Michael Brooks has never knowingly been part of another Data Breach or otherwise disclosed his Private Information to unauthorized third parties. Said differently, the only way his Private Information was disclosed to third parties was through the Data Breach.

101. The Data Breach also caused Plaintiff Michael Brooks to suffer a loss of privacy.

102. As a result of the Data Breach, Plaintiff Michael Brooks will face a substantial risk of imminent harm for the rest of his life.

103. Plaintiff Michael Brooks anticipates spending additional considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

104. The substantial risk of harm and loss of privacy from the Data Breach has caused Plaintiff Michael Brooks to suffer fear, anxiety, annoyance, inconvenience, and nuisance.

105. The Data Breach caused Plaintiff Michael Brooks to suffer a diminution in the value of his Private Information.

106. Plaintiff Michael Brooks has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

107. As a result of the Data Breach, Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private

Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain he made with Defendant by overpaying for services that were intended to be accompanied by adequate data security but were not; (e) loss of time and effort that Plaintiff Michael Brooks has had to expend in an attempt to ameliorate, mitigate, and address the consequences of the Data Breach, with such steps being taken at the direction of Defendant; and (f) continued risk to Plaintiff's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Earl Blankenship

108. Plaintiff Earl Blankenship greatly values his privacy and is very careful with his Private Information. Plaintiff Blankenship stores any documents containing Private Information in a safe and secure location or destroys such documents when they are no longer needed. Plaintiff Blankenship has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff Blankenship diligently chooses unique usernames and passwords for his various online accounts. When Plaintiff Blankenship does entrust a third-party with his Private Information, it is only because he understands such information will be reasonably safeguarded from foreseeable threats, and that he will be timely notified if his data is exposed.

109. For example, Plaintiff Blankenship provided his sensitive Private Information to Defendant in order to receive banking services and did so with the understanding that Defendant would safeguard it from unauthorized disclosure. Plaintiff Blankenship first became a customer of

Defendant's in or around June 2018. Upon information and belief, Defendant used his Private Information when providing him with its services.

110. Plaintiff Blankenship received a letter dated September 15, 2023, from Defendant notifying him of the Data Breach. The letter advised that unauthorized third parties accessed Defendant's network. The letter further advised that Plaintiff Blankenship's Private Information—including his name, date of birth, address, Social Security number,—was identified as having been "copied from [Defendant's] network."

111. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Blankenship faces, the letter offered Plaintiff Blankenship a 12-month subscription to credit monitoring services. The letter further instructed Plaintiff Blankenship to "remain vigilant by reviewing your account statements and credit reports closely." The letter additionally encouraged Plaintiff Blankenship to consider implementing the protective measures detailed in the "Steps You Can Take to Protect Your Personal Information" section of the letter.

112. As a result of the Data Breach, Plaintiff Blankenship has spent approximately 20 hours researching the Data Breach, verifying the legitimacy of the notice letter, signing up for the credit monitoring service, reviewing his bank accounts, monitoring his credit report, changing his passwords and payment account numbers, and other necessary mitigation efforts. This is valuable time Plaintiff Blankenship spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

113. As a result of the Data Breach, Plaintiff Blankenship has experienced a significant increase in spam phone calls.

114. As a result of the Data Breach, Plaintiff Blankenship received a fraudulent letter thanking him for military service, although he has never served in the military or any affiliate.

115. As a result of the Data Breach, Plaintiff Blankenship had fraudulent charges for steakhouses and an escape room in the summer of 2023, totaling $980.00. In response, Plaintiff Blankenship had to place a "red-flag" on his checking account and obtain a new debit card. In doing so, Plaintiff personally incurred charges of approximately $25.00.

116. Both the fraud and resulting costs of $25.00 are as a result of the Data Breach because (1) Plaintiff Blankenship had never previously encountered any sort of fraud; and (2) the Private Information "copied during the [Data] Breach" is the exact type of information necessary to perpetuate the fraud that Plaintiff Blankenship experienced.

117. As a result of the Data Breach, Plaintiff Blankenship has anxiety using his personal debit card and, instead, uses cash.

118. The Data Breach also caused Plaintiff Blankenship to suffer a loss of privacy.

119. As a result of the Data Breach, Plaintiff Blankenship will face a substantial risk of imminent harm for the rest of his life.

120. Plaintiff Blankenship anticipates spending additional considerable time and money on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

121. The substantial risk of harm and loss of privacy from the Data Breach has caused Plaintiff Blankenship to suffer fear, anxiety, annoyance, inconvenience, and nuisance.

122. The Data Breach caused Plaintiff Blankenship to suffer a diminution in the value of his Private Information.

123. Plaintiff Blankenship has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

124. As a result of the Data Breach, Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain he made with Defendant by overpaying for services that were intended to be accompanied by adequate data security but were not; (e) loss of time and effort that Plaintiff Blankenship has had to expend in an attempt to ameliorate, mitigate, and address the consequences of the Data Breach, with such steps being taken at the direction of Defendant; and (f) continued risk to Plaintiff's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

Plaintiff Cheryl Barefoot

125. Plaintiff Barefoot greatly values her privacy and is very careful with her Private Information. Plaintiff Barefoot has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. When Plaintiff Barefoot does entrust a third-party with her Private Information, it is only because she understands such information will be reasonably safeguarded from foreseeable threats, and that she will be timely notified if her data is exposed.

126. For example, Plaintiff Barefoot provided her sensitive Private Information to Defendant in order to receive banking services and did so with the understanding that Defendant would safeguard her Private Information from unauthorized disclosure. Plaintiff Barefoot is a current customer of Defendant. Upon information and belief, Defendant used her Private

Information when providing her with its banking services.

127. Plaintiff Barefoot received a letter dated September 15, 2023, from Defendant notifying her of the Data Breach. The letter advised that unauthorized third parties accessed Defendant's network. The letter further advised that Plaintiff Barefoot's Private Information—including her name, Social Security number, and financial account number—was identified as having been improperly accessed and obtained by unauthorized third parties.

128. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff Barefoot faces, the letter offered Plaintiff Barefoot credit monitoring and identity theft protection services through Equifax Complete™. The letter further instructed Plaintiff Barefoot to "remain vigilant by reviewing your financial account statements and credit reports for any unauthorized activity." The letter additionally encouraged Plaintiff Barefoot to consider implementing the protective measures detailed in the "Steps You Can Take to Protect Your Personal Information" section of the letter.

129. As a result of the Data Breach, Plaintiff Barefoot has spent Barefoot has spent significant time dealing with the consequences of the Data Breach including researching and verifying the legitimacy of the Data Breach upon receiving the Notice Letter. Plaintiff has spent significant time dealing with the Data Breach, valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

130. The Data Breach also caused Plaintiff Barefoot to suffer a loss of privacy.

131. As a result of the Data Breach, Plaintiff Barefoot will face a substantial risk of imminent harm for the rest of her life.

132. Plaintiff Barefoot anticipates spending additional considerable time and money on

an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

133. The substantial risk of harm and loss of privacy from the Data Breach has caused Plaintiff Barefoot to suffer fear, anxiety, annoyance, inconvenience, and nuisance.

134. The Data Breach caused Plaintiff Barefoot to suffer a diminution in the value of her Private Information.

135. Plaintiff Barefoot has a continuing interest in ensuring that her Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

136. As a result of the Data Breach, Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain she made with Defendant by overpaying for services that were intended to be accompanied by adequate data security but were not; (e) loss of time and effort that Plaintiff Barefoot has had to expend in an attempt to ameliorate, mitigate, and address the consequences of the Data Breach, with such steps being taken at the direction of Defendant; and (f) continued risk to Plaintiff's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect Private Information entrusted to it.

Plaintiff Stephen McDonald

137. Plaintiff Stephen McDonald greatly values his privacy and is very careful with his Private Information. Plaintiff McDonald stores any documents containing Private Information in a safe and secure location or destroys such documents when they are no longer needed. Plaintiff McDonald has never knowingly transmitted unencrypted sensitive Private Information over the internet or any other unsecured source. Moreover, Plaintiff McDonald diligently chooses unique usernames and passwords for his various online accounts. When Plaintiff McDonald does entrust a third-party with his Private Information, it is only because he understands such information will be reasonably safeguarded from foreseeable threats, and that he will be timely notified if his data is exposed.

138. For example, Plaintiff McDonald provided his sensitive Private Information to Defendant in order to receive banking services and did so with the understanding that Defendant would safeguard it from unauthorized disclosure. Plaintiff McDonald has been a customer of Limestone Bank since 2005. Upon information and belief, Defendant used his Private Information when providing him with its services.

139. Plaintiff McDonald received a letter dated September 15, 2023, from Defendant notifying him of the Data Breach. The letter advised that unauthorized third parties accessed Defendant's network. The letter further advised that Plaintiff McDonald's Private Information—including his name, date of birth, address, Social Security number, and financial account information—was identified as having been improperly accessed and obtained by unauthorized third parties.

140. Recognizing the present, immediate, and substantially increased risk of harm Plaintiff McDonald faces, the letter offered Plaintiff McDonald a 12-month subscription to credit

monitoring services. The letter further instructed Plaintiff McDonald to "remain vigilant by reviewing your account statements and credit reports closely." The letter additionally encouraged Plaintiff McDonald to consider implementing the protective measures detailed in the "Steps You Can Take to Protect Your Personal Information" section of the letter.

141. As a result of the Data Breach, Plaintiff McDonald has spent approximately 20 hours researching the Data Breach, verifying the legitimacy of the notice letter, signing up for the credit monitoring service, reviewing his bank accounts, monitoring his credit report, changing his passwords, addressing fraudulent login attempts, and other necessary mitigation efforts. This is valuable time Plaintiff McDonald spent at Defendant's direction and that he otherwise would have spent on other activities, including but not limited to work and/or recreation.

142. On the morning of September 25, 2023, Plaintiff received an email notice from Defendant that someone had attempted to login using his username. Plaintiff did not make this login attempt. Furthermore, Plaintiff does not use his username for his account with Defendant with any other online website.

143. On December 8, 2023, Plaintiff received an email notice from Defendant that someone successfully logged into his account. Plaintiff did not make this login.

144. Additionally, Plaintiff has experienced a surge in spam calls and texts roughly coincident with the timing of the Data Breach, indicating that hackers are already trying to take advantage of the release of his Personal Information.

145. The Data Breach also caused Plaintiff McDonald to suffer a loss of privacy.

146. As a result of the Data Breach, Plaintiff McDonald will face a substantial risk of imminent harm for the rest of his life.

147. Plaintiff McDonald anticipates spending additional considerable time and money

on an ongoing basis to try to mitigate and address the present and impending injuries caused by the Data Breach.

148. The substantial risk of harm and loss of privacy from the Data Breach has caused Plaintiff McDonald to suffer fear, anxiety, annoyance, inconvenience, and nuisance.

149. The Data Breach caused Plaintiff McDonald to suffer a diminution in the value of his Private Information.

150. Plaintiff McDonald has a continuing interest in ensuring that his Private Information, which upon information and belief, remains in Defendant's possession, is protected and safeguarded from future breaches.

151. As a result of the Data Breach, Plaintiff has also suffered injury directly and proximately caused by the Data Breach, including: (a) theft of Plaintiff's valuable Private Information; (b) the imminent and certain impending injury flowing from fraud and identity theft posed by Plaintiff's Private Information being placed in the hands of cyber criminals; (c) damages to and diminution in value of Plaintiff's Private Information that was entrusted to Defendant with the understanding that Defendant would safeguard this information against disclosure; (d) loss of the benefit of the bargain he made with Defendant by overpaying for services that were intended to be accompanied by adequate data security but were not; (e) loss of time and effort that Plaintiff McDonald has had to expend in an attempt to ameliorate, mitigate, and address the consequences of the Data Breach, with such steps being taken at the direction of Defendant; and (f) continued risk to Plaintiff's Private Information, which remains in the possession of Defendant and which is subject to further breaches so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information that was entrusted to Defendant.

CLASS ACTION ALLEGATIONS

152. Plaintiffs bring this nationwide class action on behalf of themselves and all others similarly situated under Rules 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

153. The Class that Plaintiffs seek to represent is defined as follows:

> **All persons Defendant identified as being among those individuals impacted by the Data Breach, including all who were sent a notice of the Data Breach.**

154. Excluded from the Class are Defendant's officers and directors; any entity in which Defendant has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of Defendant. Excluded also from the Class are members of the judiciary to whom this case is assigned, their families and Members of their staff.

155. Plaintiffs reserve the right to amend or modify the Class definition and/or create additional subclasses as this case progresses.

156. Numerosity. The Members of the Class are so numerous that joinder of all of them is impracticable. While the exact number of Class Members is unknown to Plaintiffs at this time, based on information and belief, the Class consists of more than 47,000 current and former clients and/or employees of Defendant whose sensitive data was compromised in Data Breach.

157. Commonality. There are questions of law and fact common to the Class, which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

a. Whether Defendant unlawfully used, maintained, lost, or disclosed Plaintiffs' and Class Members' Private Information;

b. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

c. Whether Defendant's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

d. Whether Defendant's data security systems prior to and during the Data Breach were consistent with industry standards;

e. Whether Defendant owed a duty to Class Members to safeguard their Private Information;

f. Whether Defendant breached its duty to Class Members to safeguard their Private Information;

g. Whether Defendant knew or should have known that its data security systems and monitoring processes were deficient;

h. Whether Defendant should have discovered the Data Breach sooner;

i. Whether Plaintiffs and Class Members suffered legally cognizable damages as a result of Defendant's misconduct;

j. Whether Defendant's conduct was negligent;

k. Whether Defendant's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

l. Whether Defendant breached a fiduciary duty to Plaintiffs and Class Members;

m. Whether Defendant violated the consumer protection statute invoked below;

n. Whether Defendant breach implied or express contracts with Plaintiffs and Class Members;

o. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon them by Plaintiffs and Class Members;

p. Whether Defendant failed to provide notice of the Data Breach in a timely manner, and;

q. Whether Plaintiffs and Class Members are entitled to damages, civil penalties, punitive damages, and/or injunctive relief.

158. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' information, like that of every other Class Member, was compromised in the Data Breach.

159. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of the Members of the Class. Plaintiffs' Counsel are competent and experienced in litigating data privacy class actions.

160. Predominance. Defendant has engaged in a common course of conduct toward Plaintiffs and Class Members, in that all the Plaintiffs' and Class Members' data was stored on the same computer system and unlawfully accessed in the same way. The common issues arising from Defendant's conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

161. Superiority. A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most Class

Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendant. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

162. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a Class-wide basis.

COUNT I
NEGLIGENCE
(On behalf of Plaintiffs and the Class)

163. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

164. As a condition of receiving employment or the services of Defendant or its clients, Plaintiffs and the Class were obligated to provide Defendant with their Private Information.

165. Plaintiffs and the Class entrusted their Private Information to Defendant on the premise and with the understanding that Defendant would exercise reasonable care in the protection of their Private Information.

166. Defendant has full knowledge of the sensitivity of the Private Information and the types of harm that Plaintiffs and the Class could and would suffer if the Private Information were wrongfully disclosed.

167. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the Private Information of Plaintiffs and the Class involved an unreasonable risk of harm to Plaintiffs and the Class.

168. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, configuring, maintaining, and testing Defendant's security protocols to ensure that the Private Information of Plaintiffs and the Class in Defendant's possession was adequately secured and protected.

169. Defendant also had a duty to exercise appropriate clearinghouse practices to remove job applicants' Private Information it was no longer required to retain by regulations.

170. Defendant had a duty to properly train employees to recognize phishing attempts and other common data security risks.

171. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the Private Information of Plaintiffs and the Nationwide Class.

172. Defendant's duty to use reasonable security measures arose as a result of the foreseeable harm that would occur due to its failure to exercise reasonable care.

173. Defendant was subject to an independent duty untethered to any contract between Defendant and Plaintiffs or the Class.

174. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

175. Plaintiffs and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in

collecting and storing the Private Information of Plaintiffs and the Nationwide Class, the critical importance of providing adequate security of that Private Information, and the necessity for encrypting Private Information.

176. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to encrypt the data stored on its system or to implement other reasonable industry standard measures to safeguard Private Information.

177. Plaintiffs and the Class had no ability to protect their Private Information that was in, and remains in, Defendant's possession.

178. Defendant was in an exclusive position to protect against the harm suffered by Plaintiffs and the Class as a result of the Data Breach.

179. Defendant had and continues to have a duty to adequately disclose that the Private Information of Plaintiffs and the Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their Private Information by third parties.

180. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the Private Information of Plaintiffs and the Class.

181. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the Private Information of Plaintiffs and the Class during the time the Private Information was within Defendant's possession or control.

182. Defendant improperly and inadequately safeguarded the Private Information of Plaintiffs and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

183. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of Private Information.

184. Defendant breached its duty to adequately train employees to recognize and avoid phishing attempts and other basic cybersecurity risks.

185. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Class the existence and scope of the Data Breach.

186. Defendant breached its duty to safeguard Plaintiffs' and Class Members' Private Information by failing to retain such information in an encrypted form.

187. Defendant breached its duty to safeguard Plaintiffs' and Class Members' Private Information by retaining the information for many years regardless of whether it was necessary to do so.

188. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the Private Information of Plaintiffs and the Class would not have been compromised.

189. There is a close causal connection between Defendant's failure to implement security measures to protect the Private Information of Plaintiffs and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Class. The Private Information of Plaintiffs and the Class was lost and accessed as the proximate result of Defendant's failure to

exercise reasonable care in safeguarding such Private Information by adopting, implementing, and maintaining appropriate security measures.

190. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the present and continuing consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of Plaintiffs and the Class; and (viii) present and continuing costs in terms of time, effort, and money that has been and will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

191. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

192. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

193. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
NEGLIGENCE *PER SE*
(On behalf of Plaintiffs and the Class)

194. Plaintiffs repeat and re-allege each and every allegation contained the Complaint as if fully set forth herein.

195. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant's, of failing to use reasonable measures to protect Private Information. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

196. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect Private Information and not complying with applicable industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of Private Information it obtained and stored, and the foreseeable consequences of the Data Breach for companies of Defendant's magnitude, including, specifically, the immense damages that would result to Plaintiffs and Members of the Class due to the valuable nature of the Private Information at issue in this case—including Social Security numbers.

197. Defendant's violations of Section 5 of the FTC Act constitute negligence *per se*.

198. Plaintiffs and members of the Class are within the class of persons that the FTC Act was intended to protect.

199. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of its failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

200. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and Class Members have suffered and will suffer injury, including, but not limited to, the following: (i) actual identity theft; (ii) the loss of the opportunity how their Private Information is used; (iii) the compromise, publication, and/or theft of their Private Information; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their Private Information; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information of its current and former employees and customers in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Private Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

201. Additionally, as a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and Class Members have suffered and will suffer the continued risks of exposure of their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession.

COUNT III
BREACH OF IMPLIED CONTRACT
(On behalf of Plaintiffs and the Class)

202. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

203. Defendant required Plaintiffs and Class Members to provide their Private Information as a condition of receiving its banking services. In so doing, Plaintiffs and the Class entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and the Nationwide Class if their data had been breached and compromised or stolen.

204. Plaintiffs and the Class fully performed their obligations under the implied contracts with Defendant.

205. As Plaintiffs' and Class Members' bank, Defendant had a implied duty to protect their Private Information. Notably, on its website, Defendant states:

> **We promise to protect your privacy**
>
> Peoples Bank does not share nonpublic information about you with third-party marketers outside of the Peoples family of companies without your consent, except as explained in the enclosed notice. We are permitted to disclose nonpublic personal information to nonaffiliated companies with which we have entered into joint marketing agreements (examples include mutual fund companies, broker deals, and insurance companies). We choose such non-affiliates carefully and require them to not use your private information

> other than to service you account or make you aware of special offers that may be of interest to you.
>
> …
>
> **We promise to secure your information**
>
> Security of Information is a top priority for the Peoples family of companies. We comply with federal safeguards to protect your information through physical, electronic, and procedural safeguards.

206. Despite these statements, Defendant failed to protect Plaintiffs' and Class Members' Private Information.

207. Defendant breached the implied contracts it made with Plaintiffs and the Class by (i) failing to implement technical, administrative, and physical security measures to protect the Private Information from unauthorized access or disclosure and improper (such as encryption of Social Security numbers) despite such measures being readily available, (ii) failing to limit access to the Private Information to Defendant's employees who needed such information to perform a specific job, (iii) failing to store the Private Information only on servers kept in a secure, restricted access area, and (iv) otherwise failing to safeguard the Private Information.

208. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Class have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

209. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Class are entitled to recover actual, consequential, and nominal damages.

COUNT IV
BREACH OF FIDUCIARY DUTY
(On behalf of Plaintiffs and the Class)

210. Plaintiffs repeat and re-allege each and every allegation contained the Complaint as if fully set forth herein.

211. Plaintiffs established a special relationship by virtue of Defendant accepting their Private Information in the ordinary course of providing banking services. By accepting and storing Plaintiffs' Private Information in the course of providing legal services and the scope of that relationship, Defendant accepted the duty to safeguard their Private Information.

212. Plaintiffs established a special relationship by virtue of (1) the banking relationship between Defendant and Plaintiffs; (2) Defendant accepting their Private Information; and (3) Defendant maintaining their Private Information. By accepting and continuing to store Plaintiffs' Private Information, Defendant accepted the duty as a fiduciary to safeguard Plaintiffs' Private Information.

213. As Plaintiffs' and Class Members' bank, Defendant had a special duty to protect their Private Information. Notably, on its website, Defendant states:

> **We promise to protect your privacy**
>
> Peoples Bank does not share nonpublic information about you with third-party marketers outside of the Peoples family of companies without your consent, except as explained in the enclosed notice. We are permitted to disclose nonpublic personal information to nonaffiliated companies with which we have entered into joint marketing agreements (examples include mutual fund companies, broker deals, and insurance companies). We choose such non-affiliates carefully and require them to not use your private information other than to service you account or make you aware of special offers that may be of interest to you.

…

We promise to secure your information

Security of Information is a top priority for the Peoples family of companies. We comply with federal safeguards to protect your information through physical, electronic, and procedural safeguards.

214. In light of the special relationship between Defendant and Plaintiffs and Class Members, whereby Defendant became guardians of Plaintiffs' and Class Members' Private Information, Defendant became a fiduciary by its undertaking and guardianship of the Private Information, to act primarily for the benefit of its customers, including Plaintiffs and Class Members, as follows: (1) for the safeguarding of Plaintiffs' and Class Members' Private Information; (2) to timely notify Plaintiffs and Class Members of a data breach and disclosure; and (3) to maintain complete and accurate records of what customer information (and where) Defendant did and does store.

215. Defendant had a fiduciary duty to act for the benefit of Plaintiffs and Class Members upon matters within the scope of this relationship, in particular, to keep secure the Private Information of its customers.

216. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to diligently discover, investigate, and give notice of the Data Breach in a reasonable and practicable period of time.

217. Defendant breached its fiduciary duties to Plaintiffs and Class Members by failing to encrypt and otherwise protect the integrity of the systems containing Plaintiffs' and Class Members' Private Information.

218. Defendant breached its fiduciary duties owed to Plaintiffs and Class Members by failing to timely notify and/or warn Plaintiffs and Class Members of the Data Breach.

219. Defendant breached its fiduciary duties to Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs' and Class Members' Private Information.

220. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of their Private Information; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their Private Information; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (v) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession; (vi) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (vii) the diminished value of Defendant's services they received.

221. As a direct and proximate result of Defendant's breaching its fiduciary duties, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT V
UNJUST ENRICHMENT
(On behalf of Plaintiffs and the Class)

222. Plaintiffs re-allege and incorporate by reference all other paragraphs in the Complaint as if fully set forth herein.

223. This claim is brought in the alternative to any claim for breach of contractual obligations.

224. Defendant benefited from receiving Plaintiffs' and Class Members' Private Information by its ability to retain and use that information for its own benefit. Defendant understood this benefit.

225. Defendant also understood and appreciated that Plaintiffs' and Class Members' Private Information was private and confidential, and its value depended upon Defendant maintaining the privacy and confidentiality of that information.

226. Defendant was also enriched by the fees it was paid for its services which, in part, should have been used for adequate data security.

227. Plaintiffs and Class Members were required to provide Defendant or Defendant's clients with their Private Information. In exchange, Plaintiffs and Class Members should have received adequate protection and data security for such Private Information held by Defendant.

228. Defendant knew Plaintiffs and Class Members conferred a benefit, which Defendant accepted. Defendant profited from these transactions and used the Private Information of Plaintiffs and Class Members for business purposes.

229. Defendant failed to provide reasonable security, safeguards, and protections to the Private Information of Plaintiffs and Class Members.

230. Under the principles of equity and good conscience, Defendant should not be permitted to retain money or the value of benefits belonging to Plaintiffs and Class members, because Defendant failed to implement appropriate data management and security measures mandated by industry standard.

231. Defendant wrongfully accepted and retained these benefits to the detriment of Plaintiffs and Class Members.

232. Defendant's enrichment at the expense of Plaintiffs and Class Members is and was unjust.

233. As a result of Defendant's wrongful conduct, as alleged above, Plaintiffs and Class Members are entitled to restitution and disgorgement of all profits, benefits, and other compensation obtained by Defendant, plus attorneys' fees, costs, and interest thereon.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Latasha Brooks, Michael Brooks, Earl Blankenship, Stephen McDonald, and Cheryl Barefoot pray for judgment as follows:

a) For an Order certifying this action as a Class action and appointing Plaintiffs as Class Representatives and their counsel as Class Counsel;

b) For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and Class Members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiffs and Class Members;

c) For equitable relief compelling Defendant to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

d) For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendant's wrongful conduct;

e) Ordering Defendant to pay for lifetime credit monitoring services for Plaintiffs and the Class;

f) For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

g) For an award of punitive damages, as allowable by law;

h) For an award of attorneys' fees and costs, and any other expense, including expert witness fees;

i) Pre- and post-judgment interest on any amounts awarded; and

j) Such other and further relief as this court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiffs demand a trial by jury on all claims so triable.

Date: January 19, 2024

Respectfully submitted,

/s/Terence R. Coates
Terence R. Coates (0085579)
Spencer D. Campbell (103001)
MARKOVITS, STOCK, & DEMARCO, LLC
119 E. Court St., Ste. 530
Cincinnati, Ohio 45202
Phone: (513) 651-3700
Fax: (513) 665-0219
tcoates@msdlegal.com
scampbell@msdlegal.com

Attorneys for Plaintiffs Latasha Brooks and Michael Brooks and the Proposed Class

Philip Krzeski (0095713)
CHESTNUT CAMBRONNE PA
100 Washington Avenue South, Suite 1700
Minneapolis, MN 55401
Phone: (612) 339-7300
Fax: (612) 336-2940
pkrzeski@chestnutcambronne.com

Attorney for Earl Blankenship and the Proposed Class

Michelle Kranz (0062479)
ZOLL &KRANZ, LLC
6620 West Central Avenue, Suite 100
Toledo, Ohio 43617
Tel: 419-841-9623
michelle@toledolaw.com

Carl V. Malmstrom*
WOLF HALDENSTEIN ADLER FREEMAN & HERZ LLC
111 W. Jackson Blvd., Suite 1700
Chicago, Illinois 60604
Tel: (312) 984-0000 Fax: (212) 686-0114
malmstrom@whafh.com

Attorney for Stephen McDonald and the Proposed Class

David K. Lietz*
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, LLC
5335 Wisconsin Avenue NW
Washington, D.C. 20015-2052
Telephone: (866) 252-0878
Facsimile: (202) 686-2877
dlietz@milberg.com

Attorney for Cheryl Barefoot and the Proposed Class

**pro hac vice application forthcoming*

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on January 19, 2024, the foregoing was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. Parties may access this filing through the Court's system.

/s/Terence R. Coates
Terence R. Coates (0085579)